

THE HONORABLE JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

WILLIAM A. ZIETZKE,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

CASE NO. C19-1234-JCC

ORDER

This matter comes before the Court on Petitioner's petition to quash an Internal Revenue Service summons (Dkt. No. 1) and on the Government's motion to enforce that summons (Dkt. No. 12). Having considered the parties' briefing and the relevant record, the Court finds oral argument unnecessary and DENIES Petitioner's petition. However, because the Court finds the summons overbroad, the Court ORDERS the Government to file a proposed amended summons that complies with this order. Until the Court approves an amended summons, the Court postpones ruling on the Government's motion to enforce.

I. BACKGROUND

Bitcoin¹ is a decentralized cryptocurrency that uses a distributed ledger system, or

¹ The Court draws its information about Bitcoin from the following sources: Financial Action Task Force, *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (2014); and Edward V. Murphy, M. Maureen Murphy & Michael V. Seitzinger, Cong. Research Serv., R43339, *Bitcoin: Questions, Answers, and Analysis of Legal Issues* (2015).

1 “blockchain,” to ensure the cryptocurrency’s security and integrity. To use a blockchain system,
2 a user first creates a wallet, which contains information used to move units of a cryptocurrency
3 on a blockchain. When the user downloads or purchases a wallet, software in the wallet
4 generates a private key (a large integer number). That private key is then used to mathematically
5 generate a public key (also a large integer number), which is used to create an address (a mix of
6 numbers and symbols). This address functions as the name suggests: it is the destination for a
7 cryptocurrency payment.

8 When two people agree for one person to send cryptocurrency to the other, the two reveal
9 their public addresses to one another. Because the transferor’s address is associated with their
10 public and private keys, the transferee can confirm the transferor’s ownership of the transferred
11 cryptocurrency by verifying that the transferor’s private key, public key, and address correspond.
12 And once the cryptocurrency is transferred, the transferee can spend or withdraw the
13 cryptocurrency with their own private key, which will now be associated with that
14 cryptocurrency.

15 Although cryptocurrency transactions can occur directly between individuals, those
16 transactions are often handled through digital currency exchanges. Digital currency exchanges
17 are businesses that hold large amounts of traditional and cryptocurrency, allowing them to
18 facilitate third-party transactions of traditional currency for cryptocurrency. To help facilitate
19 such transactions, these businesses also provide hosted wallet services.

20 As with many things in life, cryptocurrency transactions have tax consequences. In 2014,
21 the IRS set forth its position on those consequences in IRS Notice 2014-21, 2014-16 I.R.B. 938.
22 Notice 2014-21 states, “virtual currency is treated as property. General tax principles applicable
23 to property transactions apply to transactions using virtual currency.” Cryptocurrency is,
24 therefore, taxed according to the gain or loss a taxpayer realizes when they sell or exchange
25 cryptocurrency. *Id.* A taxpayer’s gain or loss is determined by looking at the difference between
26 the cryptocurrency’s basis and the amount the taxpayer receives in exchange for the currency. *Id.*

1 The basis, in turn, “is the fair market value of the currency in U.S. dollars as of the date of
2 receipt.” *Id.* And the cryptocurrency’s fair market value is usually determined by the price at
3 which the taxpayer purchases the cryptocurrency. *Id.*

4 Petitioner attempted to navigate the tax consequences of cryptocurrency transactions
5 when he self-prepared his 2016 tax return using Turbo Tax. (Dkt. No. 23 at 2.) In his 2016
6 return, Petitioner reported Schedule D long-term capital gains of \$104,482. (Dkt No. 19 at 2–3.)
7 Petitioner calculated the \$104,482 figure by including two Bitcoin transactions that he listed as
8 having occurred in 2016. (*Id.*) According to Petitioner, these transactions did not actually occur
9 in 2016. (*Id.* at 3.) However, Petitioner claims that he realized his mistake only after his Certified
10 Public Accountant David Rumsey, whom Petitioner hired in 2017 to help him prepare for
11 retirement, reviewed his tax returns and caught Petitioner’s error. (*Id.*) Petitioner subsequently
12 filed an amended return on August 14, 2017, that omitted the two transactions and thereby
13 reduced his long-term capital gains in 2016 from \$104,482 to \$410. (*Id.*) If correct, this reduction
14 would entitle Petitioner to a \$15,475 refund. (*Id.*)

15 Petitioner’s refund request caught the IRS’s attention, and on June 25, 2018, IRS
16 Revenue Agent Amanda Snow sent Petitioner a letter informing him that the IRS was examining
17 his 2016 tax return. (Dkt. No. 19-1 at 18.) In the months that followed, Petitioner provided the
18 IRS with information about his Bitcoin holdings and transactions. (*See* Dkt. Nos. 13 at 3–5, 19 at
19 4–26.) Petitioner informed the IRS that he had two separate groups of Bitcoin holdings. (Dkt.
20 No. 13 at 4–5.) The first group consisted of his personal holdings that he managed through
21 Armory wallet software. (*Id.*) The second group allegedly consisted of Bitcoins held in wallets
22 hosted by Coinbase, a currency exchange, and Purse.io, a hosted wallet platform that operates as
23 a Bitcoin-to-Amazon.com item exchange. (*Id.*) Petitioner told the IRS that these latter holdings
24 originated when Petitioner deposited U.S. dollars from a personal bank account into a Coinbase
25 account and then transferred funds from that account to his Purse.io account. (*Id.* at 5.)

26 Although Petitioner initially told the IRS that he used only two hosted wallet platforms,

1 the IRS discovered that Petitioner also used Bitstamp, another currency exchange. (Dkt. No. 13
2 at 5–6.) In addition, the IRS learned that Petitioner used Bitstamp to conduct at least one Bitcoin
3 transaction in 2016. (Dkt. No. 23 at 2.) Upon learning of this transaction, the IRS issued a
4 summons to Bitstamp. (Dkt. No. 1-1 at 3–15.) The summons directs Bitstamp to produce for
5 examination books, records, papers, and other data relating to Petitioner’s holdings with
6 Bitstamp. (*See id.* at 12–15.) The requested data includes Petitioner’s public keys and blockchain
7 addresses. (*Id.* at 13.) It does not include Petitioner’s private keys. (*See id.* at 12–15.)

8 On June 27, 2019, Petitioner filed a petition to quash the summons that the IRS served on
9 Bitstamp. (Dkt. No. 1.) The IRS subsequently moved for the Court to enforce its summons and to
10 deny the petition to quash. (Dkt. No. 12.)

11 **II. DISCUSSION**

12 Petitioner asks the Court to quash the Bitstamp summons for six reasons: (1) the IRS
13 issued the summons in bad faith; (2) the IRS seeks information that is irrelevant to its audit of
14 Petitioner’s 2016 amended return; (3) the IRS already possesses the information that it seeks
15 from Bitstamp; (4) the IRS failed to follow the administrative steps required by the United States
16 Code for issuance and service of a summons; (5) the summons violates Petitioner’s reasonable
17 expectation of privacy in Bitstamp’s records; and (6) the Government cannot guarantee the
18 security of any records that it receives from Bitstamp. (*See* Dkt. No. 23 at 12–24.) Although five
19 of Petitioner’s arguments lack merit, he is correct that the summons is overbroad because it seeks
20 both relevant and irrelevant material.

21 **A. Legal Standard**

22 Congress requires that the IRS investigate the tax liability of persons who may be liable
23 to pay an internal revenue tax. 26 U.S.C. § 7601. To help the IRS conduct such investigations,
24 Congress enacted 26 U.S.C. § 7602(a), which gives the IRS the power to issue administrative
25 summons. “The § 7602 summons is critical to the investigative and enforcement functions of the
26 IRS.” *United States v. Arthur Young & Co.*, 465 U.S. 805, 814 (1984). The IRS’s power to issue

1 summons has, therefore, been construed broadly in the IRS’s favor. *See United States v. Euge*,
2 444 U.S. 707, 714–15 (1980).

3 The breadth of the IRS’s power under § 7602(a) is reflected in the test for determining
4 the validity of a summons. *See United States v. Clarke*, 573 U.S. 248, 254–55 (2014). Under that
5 test, the Government must first present a *prima facie* case for enforcement. *United States v.*
6 *Powell*, 379 U.S. 49, 57–58 (1964). The Government establishes a *prima facie* case by showing
7 that (1) the IRS issued the summons for a legitimate purpose; (2) the summoned data may be
8 relevant to that purpose; (3) the IRS does not already possess the summoned data; and (4) the
9 IRS followed the administrative steps required by the United States Code for issuance and
10 service of a summons. *Id.* The Government’s burden at this stage is “slight.” *Fortney v. United*
11 *States*, 59 F.3d 117, 120 (9th Cir. 1995). Consequently, the Government usually meets its burden
12 by introducing a sworn declaration of the revenue agent who issued the summons stating that the
13 *prima facie* case requirements have been met. *Id.*

14 If the Government establishes a *prima facie* case, then the burden shifts to the petitioning
15 taxpayer to show that the IRS is attempting to abuse the court’s process or is lacking in good
16 faith. *United States v. Dynavac, Inc.*, 6 F.3d 1407, 1414 (9th Cir. 1993). The burden on the
17 taxpayer to disprove the IRS’s assertions is “heavy.” *Id.* (quoting *United States v. Abrahams*, 905
18 F.2d 1276, 1280 (9th Cir. 1990)).

19 **B. The *Powell* Requirements**

20 Petitioner argues that the Government did not meet any of the *Powell* requirements. (*See*
21 Dkt. No. 23 at 12–19.) For the reasons explained below, the Court concludes that the
22 Government has met all but the second *Powell* requirement. With respect to the second
23 requirement, the Court concludes that, as written, the Bitstamp summons seeks irrelevant
24 material because it lacks a temporal limitation.

25 1. Legitimate Purpose

26 In her sworn declaration, Ms. Snow articulates a legitimate purpose for the IRS’s

1 decision to serve a summons on Bitstamp. The IRS may issue a summons for a “civil tax
2 collection purpose.” *United States v. Stuckey*, 646 F.2d 1369, 1375 (9th Cir. 1981). In addition,
3 the IRS “can investigate merely on suspicion that the law is being violated, or even just because
4 it wants assurances that it is not.” *Powell*, 379 U.S. at 57 (quoting *United States v. Morton Salt*
5 *Co.*, 338 U.S. 632, 642–43 (1950)). And according to Ms. Snow, that is exactly what is
6 happening here: the IRS wishes to determine the tax implications of Petitioner’s 2016 transaction
7 involving his Bitstamp holdings and to figure out if Petitioner engaged in similar transactions
8 that year. (*See* Dkt. No. 13 at 5–7.) The IRS therefore served a summons on Bitstamp to
9 ascertain the number of Petitioner’s Bitcoin transactions in 2016, what Bitcoins Petitioner used
10 to conduct those transactions, when Petitioner acquired the relevant Bitcoins, and how Petitioner
11 acquired those Bitcoins. (*See id.*) Ms. Snow’s representations satisfy the Government’s “slight”
12 burden for showing that the IRS served the summons for a legitimate purpose. *See Fortney*, 59
13 F.3d at 120.

14 Notwithstanding Ms. Snow’s stated rationale, Petitioner claims that the IRS served a
15 summons on Bitstamp in a bad-faith attempt to “obtain details of his bitcoin **holdings**.” (*See* Dkt.
16 No. 23 at 1–2) (emphasis in original). Petitioner argues that the IRS’s bad faith is evident from
17 the following: (1) the IRS has refused to accept Petitioner’s representation that Bitstamp has no
18 information relevant to the IRS’s audit; (2) the audit has taken a long time; and (3) there is a low
19 amount of money at stake. (*See id.* at 13–16.) But Petitioner’s arguments amount to no more than
20 speculation. For example, while it is possible that the IRS has taken a long time to audit
21 Petitioner’s \$15,475 refund claim because it secretly wishes to gather information about his
22 wealth, it is equally possible that the IRS is just being thorough. After all, the IRS is required by
23 Congress to investigate persons who may owe taxes—regardless of the amount. *See* 26 U.S.C.
24 § 7601. Similarly, the IRS need not accept a person’s assertion that they complied with all
25 relevant tax laws; it “can investigate merely on suspicion that the law is being violated, or even
26 just because it wants assurances that it is not.” *Powell*, 379 U.S. at 57 (quoting *Morton Salt Co.*,

338 U.S. at 642–43). Therefore, absent some actual evidence of bad faith, Petitioner has failed to carry his “heavy” burden for showing that the IRS gave a pretextual reason for serving Bitstamp.² *See Dynavac, Inc.*, 6 F.3d at 1414 (quoting *Abrahams*, 905 F.2d at 1276).

2. Relevance

In addition to needing a legitimate purpose, a summons must seek records that “may be relevant” to the purpose of the summons. 26 U.S.C. § 7602(a)(1); *Powell*, 379 U.S. at 57–58. The key word is “may.” *Arthur Young & Co.*, 465 U.S. at 814. As the Supreme Court has explained,

The language “may be” [in § 7602(a)(1)] reflects Congress’ express intention to allow the IRS to obtain items of even *potential* relevance to an ongoing investigation The purpose of Congress is obvious: the Service can hardly be expected to know whether such data will in fact be relevant until it is procured and scrutinized.

Id. Thus, the IRS does not need to guarantee that the records it seeks will be relevant; it is enough that they “might . . . thro[w] light upon the correctness of the return.” *Id.* at 813 n.11 (quoting *United States v. Wyatt*, 637 F.2d 293, 300 (5th Cir. 1981)).

Here, the summons at issue seeks records that may be relevant to the IRS’s audit of Petitioner’s 2016 amended return. To determine whether Petitioner correctly amended his 2016 return, the IRS must determine how many Bitcoin transactions Petitioner engaged in that year. (*See* Dkt. No. 13 at 5.) In addition, the IRS must figure out Petitioner’s basis for each transaction that did occur. *See* Notice 2014-21, 2014-16 I.R.B. 938; (Dkt. No. 13 at 6). These inquiries

² Petitioner argues that even if he currently lacks evidence of bad faith, his outstanding Freedom of Information Act request might reveal such evidence. (*See* Dkt. No. 23 at 16.) Petitioner therefore asks the Court to defer deciding this case until the IRS responds to his FOIA request. (*See id.*) Yet, in the 18 months since Petitioner first made the request, it does not appear that Petitioner ever sought to compel the IRS to respond using the procedures set forth in 5 U.S.C. § 552. (*See* Dkt. No. 19-3 at 23.) And Petitioner cites no authority for the idea that if the IRS does not respond to a FOIA request, then a district court can or should delay deciding whether to enforce an IRS summons. (*See* Dkt. No. 23 at 16.) Given that lack of authority, the Court declines to delay its decision and holds that Petitioner has failed to demonstrate that the IRS acted in bad faith when it issued the Bitstamp summons.

1 require that the IRS look at the records of exchanges that Petitioner used to hold Bitcoins. (*See*
2 Dkt. No. 13 at 5–7.) Bitstamp is one such exchange, and the records the IRS seeks from the
3 company might shed light on Petitioner’s Bitcoin transactions in 2016. (*See id.*)

4 Despite the relevance of Bitstamp’s records, Petitioner argues that the summons is
5 overbroad because it lacks a temporal limitation. (*See* Dkt. Nos. 1 at 14–16, 23 at 16–18.) In
6 making that argument, Petitioner emphasizes that a summons must be “no broader than
7 necessary to achieve its purpose.” (*See* Dkt. No. 1 at 16) (quoting *United States v. Bisceglia*, 420
8 U.S. 141, 151 (1975)). This language does not, however, impose any sort of narrow tailoring
9 requirement. *See Tiffany Fine Arts, Inc. v. United States*, 469 U.S. 310, 23 (1985) (“We have
10 never held . . . that the IRS must conduct its investigations in the least intrusive way possible.
11 Instead, the standard is one of relevance.”). Rather, the language stands for the simple
12 proposition that a district court may narrow a summons when the summons seeks both relevant
13 and irrelevant material. *See United States v. Richards*, 631 F.2d 341, 345–46 (4th Cir. 1980)
14 (concluding modification of summons was appropriate because the summons as written asked for
15 information relating to a corporation’s payments that may have been illegal but did not affect the
16 corporation’s tax liability). Thus, the core question here is whether the IRS’s request for pre-
17 2016 records from Bitstamp asks for material that is irrelevant to the IRS’s investigation of
18 Petitioner’s 2016 amended return. *See United States v. Goldman*, 637 F.2d 664, 667 (9th Cir.
19 1980) (affirming district court’s conclusion that records from years 1970–1972 were irrelevant
20 because they could not impact petitioner’s tax liability in the years the IRS was investigating).

21 The answer to that question is yes. While the IRS is correct that it “must have
22 information for prior years in order to properly calculate any resulting loss or gain [in 2016],”
23 (*see* Dkt. No. 12 at 13), the information that the IRS needs is the price Petitioner paid for
24 Bitcoins he sold in 2016, *see* Notice 2014-21, 2014-16 I.R.B. 938 (explaining that the basis for
25 cryptocurrency is usually the purchase price). Yet, the summons asks for far more than that. (*See*
26 Dkt. No. 1-1 at 12–14.) Among other things, it requests “[a]ll account history information (on-

1 chain and off-chain) for transactions or events relating to any Covered Accounts.” (*Id.* at 13.)
2 This request would require Bitstamp to produce information relating to Petitioner’s Bitcoin sales
3 prior to 2016—even though such sales could not impact the gain or loss Petitioner realized if he
4 sold Bitcoins in 2016. In this way, the summons requests information that is irrelevant to the
5 IRS’s stated purpose of auditing Petitioner’s 2016 amended return. The summons is therefore
6 overbroad. *See Goldman*, 637 F.2d at 667.

7 3. Documents the IRS Already Possesses

8 The third *Powell* requirement obligates the IRS to seek information that it does not
9 already possess. 379 U.S. at 57–58. Ms. Snow states that the IRS does not already have the
10 documents and information demanded in the Bitstamp summons. (*See* Dkt. No. 13 at 2.)
11 Petitioner disagrees, arguing that “he has provided the IRS with all of the information related to
12 the one and only transaction that he engaged in with Bitstamp during 2016.” (*See* Dkt. No. 23 at
13 18.) But the IRS is not required to rely on Petitioner’s claim that he has provided the agency with
14 everything it needs to know. Consequently, the Government has met the third *Powell*
15 requirement.

16 4. The IRS’s Compliance with Required Administrative Steps

17 To meet the fourth *Powell* requirement, the IRS must satisfy all administrative steps
18 required by the United States Code. 379 U.S. at 57–58. If a taxpayer does not contest that the
19 IRS complied with an administrative requirement, then the Government satisfies its burden under
20 *Powell* by submitting “[a] sworn declaration . . . that the *Powell* requirements have been met.”
21 *Fortney*, 59 U.S. at 120 (quoting *Dynavac, Inc.*, 6 F.3d at 1414). Because that burden is “slight”
22 and summons proceedings are “summary in nature,” the sworn declaration need not address
23 every administrative requirement in the Code. *See Clarke*, 573 U.S. at 254. It is enough that the
24 declaration states generally that the IRS complied with all administrative requirements. *See id.*;
25 *Fortney*, 59 U.S. at 120.

26 Here, Petitioner does not argue in any properly filed motion that the IRs failed to satisfy

1 an administrative requirement.³ (*See generally* Dkt. Nos. 1, 23.) In addition, Ms. Snow states that
2 the administration complied with all administrative requirements. (*See* Dkt. No. 13 at 2.) As a
3 result, the Government has met the fourth *Powell* requirement.

4 **C. Petitioner’s Privacy Concerns**

5 In addition to arguing that the Government has not met the *Powell* requirements,
6 Petitioner also asks the Court to quash the Bitstamp summons because of two privacy concerns.
7 First, Petitioner argues that it would “violat[e] . . . [his] right to privacy” if the IRS gains access
8 to his public keys or addresses. (*See* Dkt. No. 1 at 17.) Second, Petitioner asserts that “the IRS is
9 unable to adequately secure such highly sensitive information.” (*See id.* at 8.) Neither argument
10 has merit.

11 1. Petitioner’s Right to Privacy

12 The Fourth Amendment protects people from “unreasonable searches and seizures” of
13 “their persons, houses, papers, and effects.” U.S. Const. amend. IV. Over time, the Supreme
14 Court has defined “search” in two distinct ways. The first establishes a “baseline” of Fourth
15 Amendment protections: the Government engages in a search when it physically intrudes on a
16 constitutionally protected area to obtain information. *See Florida v. Jardines*, 569 U.S. 1, 5
17 (2013). The second definition expands Fourth Amendment protections beyond notions of
18 property. *See Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). Under that definition, the
19 Government also engages in a search if it intrudes on a person’s reasonable expectation of
20 privacy. *See id.*

21
22 ³ In a “motion for leave to file a short supplement” to his response, Petitioner argues for the first
23 time that the IRS failed to comply with the advance notice requirement in 26 U.S.C. §
24 7602(c)(1). (*See* Dkt. No. 30 at 1.) This motion is, in reality, an attempt by Petitioner to file a
25 surreply. But a surreply “shall be strictly limited to addressing [a] request to strike,” and “a
26 surreply filed for any other reason shall not be considered.” W.D. Wash. Local Civ. R. 7(g)(2).
Petitioner’s motion is plainly not a request to strike. Consequently, the Court DENIES
Petitioner’s motion for leave to file a supplemental response to the Government’s motion to
enforce the Bitstamp summons.

1 In *United States v. Miller*, 425 U.S. 435, 440–43 (1976), the Supreme Court held that a
2 person lacks a reasonable expectation of privacy in a bank’s records pertaining to the person. The
3 *Miller* Court based its holding on two distinct grounds. First, citing its third-party exposure
4 cases, the Supreme Court stated that “the Fourth Amendment does not prohibit the obtaining of
5 information revealed to a third party and conveyed by him to Government authorities.” *Id.* at 443
6 (citing *United States v. White*, 401 U.S. 745, 752 (1971); *Hoffa v. United States*, 385 U.S. 293,
7 302 (1966); *Lopez v. United States*, 373 U.S. 427 (1963)). Second, the Supreme Court observed
8 that bank records “[were] not the respondent’s ‘private papers’” but were instead “the business
9 records of the banks.” *Id.* at 440. Accordingly, the Government could subpoena those records
10 without infringing on the respondent’s Fourth Amendment rights. *Id.* at 444.

11 In *Carpenter v. United States*, 138 S. Ct. 2206, 2217 & n.3 (2018), the Supreme Court
12 distinguished *Miller* and held that a person has a reasonable expectation of privacy in seven days
13 of historical cell-site location information (CSLI) produced by their cell phone. Although CSLI
14 is revealed to and owned by wireless carriers, the *Carpenter* majority held that these factors did
15 not necessarily render a person’s expectation of privacy in CSLI unreasonable. *Id.* at 2219.
16 Instead, the majority concluded that it must consider “‘the nature of the particular documents
17 sought’ to determine whether ‘there is a legitimate “expectation of privacy” concerning their
18 contents.’” *Id.* (quoting *Miller*, 425 U.S. at 442). The nature of CSLI is especially revealing, the
19 majority reasoned, because “time-stamped data provides an intimate window into a person’s life,
20 revealing not only his particular movements, but through them his ‘familial, political,
21 professional, religious, and sexual associations.’” *Id.* at 2217–18 (quoting *United States v. Jones*,
22 565 U.S. 400, 415 (2012)). And given CSLI’s revealing nature, the majority held that people
23 retain an “expectation of privacy in the whole of their physical movements” even after they give
24 data about those movements to wireless carriers. *Id.* at 2219.

25 Petitioner asks the Court to extend *Carpenter* to this case and hold that Petitioner has a
26 reasonable expectation of privacy in Bitstamp’s cryptocurrency records pertaining to him. (*See*

1 Dkt. No. 23 at 19.) This request places the Court in the somewhat unenviable position of trying
2 to reconcile *Miller* and *Carpenter* to determine what makes a person’s expectation of privacy in
3 bank records less reasonable than their expectation of privacy in CSLI. Unfortunately, lower
4 courts trying to make that determination were given little guidance by the *Carpenter* majority.
5 For while the majority said that “[t]here is a world of difference” between bank records and
6 CSLI, *Carpenter*, 138 S. Ct. at 2219, the majority chose to not respond to Justice Kennedy’s
7 observation that bank records can reveal “how much money [persons] make; the political and
8 religious organizations to which they donate; whether they have visited a psychiatrist, plastic
9 surgeon, abortion clinic, or AIDs treatment center; whether they go to gay bars or straight ones;
10 and who are their closest friends and family members,” *id.* at 2232 (Kennedy, J., dissenting).

11 Despite this lack of guidance, the *Carpenter* majority did make two points that are
12 instructive here. First, the majority stated that its decision was “a narrow one” that “did not
13 disturb the application of . . . *Miller*.” *Id.* at 2220 (majority opinion). The Court takes this
14 statement seriously, and it will extend *Carpenter* to new circumstances only if they directly
15 implicate the privacy concerns that animated the majority. Second, the majority was
16 overwhelmingly concerned with “*Carpenter*’s anticipation of privacy in his physical location.”
17 *See id.* at 2217–20. In other words, *Carpenter* was about surveillance. *See id.* (discussing the
18 Supreme Court’s prior surveillance cases).

19 These two points compel the conclusion that *Carpenter* does not apply here. To begin
20 with, this case does not involve surveillance of any kind. It involves a request for financial
21 records. (*See* Dkt. No. 1.) In addition, those financial records were exposed to and are owned by
22 a third party. (*See* Dkt. No. 1-1 at 3–15.) Petitioner’s privacy interest in the requested records is,
23 therefore, greatly diminished. *See Miller*, 425 U.S. at 442–43. And most importantly, the
24 requested records do not implicate Petitioner’s “anticipation of privacy in his physical location”
25 or his “expectation of privacy in the whole of his physical movements.” *Carpenter*, 138 S. Ct. at
26 2217, 2219. At most, the records might reveal Petitioner’s “buying and spending history and

1 [his] wealth.” (See Dkt. No. 23 at 21–22.) But that was equally true of the bank records in
2 *Miller*—records that did not receive Fourth Amendment protection even though, as Justice
3 Kennedy pointed out, those records can reveal “troves of intimate information.” See *Carpenter*,
4 138 S. Ct. at 2232 (Kennedy, J., dissenting) (citing *Miller*, 425 U.S. at 451 (Brennan, J.,
5 dissenting)).

6 Because Bitstamp’s records do not implicate the privacy concerns at issue in *Carpenter*,
7 Petitioner lacks a legitimate expectation of privacy in those records. Consequently, the IRS’s
8 request for those records does not infringe upon Petitioner’s Fourth Amendment rights. See
9 *Miller*, 425 U.S. at 441.

10 5. The Security of the IRS’s Records

11 Petitioner argues that the Court should quash the Bitstamp summons because the
12 Government cannot adequately guarantee the security of any records that it receives from
13 Bitstamp. (See Dkt. Nos. 1 at 8–9, 23 at 22–24.) This is, to put it bluntly, not a legal argument.
14 Petitioner cites no law or case suggesting that a court may quash an IRS summons based on
15 concerns about the Government’s security practices. (See Dkt. Nos. 1 at 8–9, 23 at 22–24.)
16 Petitioner should direct his concerns over such practices to the branches of government that are
17 best positioned and constitutionally empowered to address those concerns: Congress and the
18 Executive.

19 **III. CONCLUSION**

20 For the foregoing reasons, the Court ORDERS as follows:

- 21 1. Petitioner’s motion for leave to file a short supplement (Dkt. No. 30) is DENIED.
- 22 2. Petitioner’s petition to quash (Dkt. No. 1) is DENIED.
- 23 3. The Government is ORDERED to file a proposed amended summons within 14 days of
24 this order. The amended summons must modify requests four through nine so that those
25 requests demand information relating only to transactions that Petitioner made in 2016.
26 Those requests may ask for information prior to 2016 only to the extent that the

1 information is relevant to determining the tax implications of transactions in 2016. The
2 IRS does not need to modify its other requests.

- 3 4. If Petitioner wishes to oppose the proposed amended summons, he must do so within
4 seven days of the Government filing the proposed amended summons. Petitioner may
5 oppose the proposed amended summons only insofar as it requests information that is not
6 relevant to the tax implications of transactions in 2016.

7 DATED this 25th day of November 2019.

8
9
10 

11 John C. Coughenour
12 UNITED STATES DISTRICT JUDGE
13
14
15
16
17
18
19
20
21
22
23
24
25
26